# Cybersecurity in Automated Food Manufacturing Systems Training Course

Professional Development Training Course Outline

| | | | |
|---|---|---|---|
| **Category** | Food processing and Technology | **Duration** | 5 Days |
| **Base Fee** | $1,500 USD | **Delivery Mode** | Online / On-site Hybrid |

## Course Introduction

The rapid adoption of automation and digital transformation in the food manufacturing sector has led to increased reliance on interconnected systems, industrial control systems (ICS), and IoT-enabled devices. While automation enhances productivity, efficiency, and quality control, it also exposes the industry to heightened cybersecurity vulnerabilities. Cyberattacks targeting automated systems can disrupt production, compromise food safety, and cause severe economic and reputational damage. Addressing cybersecurity threats in this environment is critical to ensuring the resilience of manufacturing systems and the safety of consumers.

Cybersecurity in Automated Food Manufacturing Systems Training Course equips participants with practical knowledge and hands-on strategies to safeguard smart factories and digital infrastructures. The program combines global cybersecurity frameworks, food industry best practices, and real-world case studies. Participants will explore cyber risk management, data integrity, operational technology (OT) defense, regulatory compliance, and emerging technologies, ensuring they are fully prepared to prevent, detect, and respond to cyber incidents in automated food manufacturing environments.

## Programme Curriculum

**Cybersecurity in Automated Food Manufacturing Systems Training Course**

**Introduction**

The rapid adoption of automation and digital transformation in the food manufacturing sector has led to increased reliance on interconnected systems, industrial control systems (ICS), and IoT-enabled devices. While automation enhances productivity, efficiency, and quality control, it also exposes the industry to heightened cybersecurity vulnerabilities. Cyberattacks targeting automated systems can disrupt production, compromise

food safety, and cause severe economic and reputational damage. Addressing cybersecurity threats in this environment is critical to ensuring the resilience of manufacturing systems and the safety of consumers.

Cybersecurity in Automated Food Manufacturing Systems Training Course equips participants with practical knowledge and hands-on strategies to safeguard smart factories and digital infrastructures. The program combines global cybersecurity frameworks, food industry best practices, and real-world case studies. Participants will explore cyber risk management, data integrity, operational technology (OT) defense, regulatory compliance, and emerging technologies, ensuring they are fully prepared to prevent, detect, and respond to cyber incidents in automated food manufacturing environments.

**Course Objectives**

1. Understand the fundamentals of cybersecurity in automated food manufacturing systems.
2. Analyze the intersection of industrial automation, IoT, and cybersecurity.
3. Evaluate vulnerabilities in industrial control systems (ICS) and operational technology (OT).
4. Apply global cybersecurity frameworks and standards to food manufacturing.
5. Enhance digital resilience with AI-driven cybersecurity solutions.
6. Develop risk assessment strategies for automated production lines.
7. Strengthen supply chain cybersecurity for food safety assurance.
8. Design incident response and disaster recovery strategies for food plants.
9. Implement data integrity and secure communication in smart factories.
10. Leverage blockchain and predictive analytics for food cybersecurity.
11. Monitor real-time cyber threats using SOC tools and industrial monitoring systems.
12. Apply compliance frameworks such as ISO 27001, NIST, and FDA FSMA guidelines.
13. Integrate cybersecurity culture and workforce awareness training.

**Organizational Benefits**

1. Strengthened protection of automated manufacturing systems against cyber threats.
2. Improved compliance with global food safety and cybersecurity regulations.
3. Enhanced resilience and disaster recovery capabilities.
4. Reduced downtime and production losses caused by cyber incidents.
5. Increased stakeholder trust and consumer safety assurance.
6. Optimized integration of cybersecurity with Industry 4.0 technologies.
7. Boosted employee readiness to identify and respond to threats.
8. Better supply chain security management.
9. Advanced decision-making with real-time threat intelligence.
10. Long-term cost savings through proactive cybersecurity measures.

**Target Audiences**

1. Food Manufacturing IT Security Professionals
2. Plant Managers and Production Supervisors
3. Quality Assurance and Compliance Officers
4. Supply Chain Managers in Food Manufacturing
5. Cybersecurity Analysts and Engineers
6. Food Industry Regulators and Auditors
7. Operations and Maintenance Technicians
8. Industrial Automation and Control Specialists

**Course Duration**: 5 days

**Course Modules**

**Module 1: Introduction to Cybersecurity in Food Manufacturing**

- Fundamentals of cybersecurity in the food industry
- Cyber risks in automated food systems
- Role of industrial automation and IoT
- Global threat landscape in manufacturing
- Regulatory drivers for cybersecurity adoption
- Case study: Ransomware attack in a food processing plant

**Module 2: Industrial Control Systems (ICS) and OT Security**

- Overview of ICS and OT environments
- Identifying vulnerabilities in control systems
- Threats to programmable logic controllers (PLC)
- Secure configuration of industrial networks
- Monitoring and logging in OT environments
- Case study: Stuxnet implications for food automation

**Module 3: Cyber Risk Assessment and Management**

- Risk analysis frameworks for food automation
- Identifying critical assets and processes
- Cybersecurity maturity models
- Risk prioritization and mitigation strategies
- Integration with enterprise risk management
- Case study: Risk assessment in dairy automation systems

**Module 4: Cybersecurity Standards and Compliance**

- ISO 27001 in food manufacturing
- NIST Cybersecurity Framework application
- FDA FSMA cybersecurity requirements
- EU regulations on digital security in food industries
- Aligning compliance with operational strategies
- Case study: Compliance audit in a smart bakery plant

**Module 5: Data Integrity and Secure Communications**

- Importance of data integrity in production
- Secure data transfer protocols
- Encryption for food manufacturing data
- Protecting recipe and process data
- Preventing data manipulation in IoT systems
- Case study: Data breach in beverage automation systems

**Module 6: Incident Response and Business Continuity**

- Developing incident response frameworks
- Role of SOC in food manufacturing
- Steps for effective cyber incident management

- Disaster recovery strategies for food plants
- Business continuity planning and resilience
- Case study: Cyber incident recovery in a frozen food facility

**Module 7: Emerging Technologies in Cybersecurity**

- AI-driven security solutions
- Predictive analytics for threat detection
- Role of blockchain in food traceability and security
- Machine learning for anomaly detection
- Cloud security in food automation systems
- Case study: Blockchain securing supply chain in poultry

**Module 8: Building Cybersecurity Culture in Food Manufacturing**

- Workforce training and awareness
- Role of leadership in cyber resilience
- Insider threats and mitigation strategies
- Integrating cybersecurity into daily operations
- Encouraging reporting and continuous improvement
- Case study: Workforce training impact in a global food brand

**Training Methodology**

- Interactive lectures and expert-led discussions
- Hands-on simulation exercises in ICS and OT environments
- Real-world case study analysis from global food manufacturers
- Group activities and cybersecurity scenario workshops
- Assessment through quizzes, group projects, and presentations

**Register as a group from 3 participants for a Discount**

**Send us an email: info@fineskilltrainingcenter.org or call** *+254769199797*

***Certification***

*Upon successful completion of this training, participants will be issued with a globally- recognized certificate.*

***Tailor-Made Course***

*We also offer tailor-made courses based on your needs.*

**Key Notes**

**a.** The participant must be conversant with English.

**b.** Upon completion of training the participant will be issued with an Authorized Training Certificate

**c.** Course duration is flexible and the contents can be modified to fit any number of days.

**d.** The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

**e.** One-year post-training support Consultation and Coaching provided after the course.

**f.** Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

## Upcoming Scheduled Sessions

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **23 Nov 2026** | 27 Nov 2026 | Online | $1,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $1,500 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $3,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $3,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $4,500 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |

Ready to enroll or request a customized program? Book online or contact us:

**Register Online Now**

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com